

Kochen-Specker sets and Hadamard matrices

Petr Lisoněk*

Department of Mathematics
Simon Fraser University
Burnaby, BC, V5A 1S6
Canada

plisonek@sfu.ca

March 3, 2017

Abstract

We introduce a new class of complex Hadamard matrices which have not been studied previously. We use these matrices to construct a new infinite family of parity proofs of the Kochen-Specker theorem. We show that the recently discovered simple parity proof of the Kochen-Specker theorem is the initial member of this infinite family.

1 Introduction

Kochen-Specker theorem is an important result in quantum mechanics [5]. It demonstrates the contextuality of quantum mechanics, which is one of its properties that may become crucial in quantum information theory [4]. In this paper we focus on proofs of Kochen-Specker theorem that are given by showing that, for $n \geq 3$, there does not exist a function $f : \mathbb{C}^n \rightarrow \{0, 1\}$ such that for every orthogonal basis B of \mathbb{C}^n there exists *exactly one* vector $x \in B$ such that $f(x) = 1$ (where \mathbb{C}^n denotes the n -dimensional vector space over the field of complex numbers). This particular approach has been used in many publications, see for example [1, 7, 8, 9] and many references cited therein. The following definition formalizes one common way of constructing such proofs.

*Research was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Definition 1.1. We say that $(\mathcal{V}, \mathcal{B})$ is a *Kochen-Specker pair* in \mathbb{C}^n if it meets the following conditions:

- (1) \mathcal{V} is a finite set of vectors in \mathbb{C}^n .
- (2) $\mathcal{B} = (B_1, \dots, B_k)$ where k is odd, and for all for $i = 1, \dots, k$ we have that B_i is an orthogonal basis of \mathbb{C}^n and $B_i \subset \mathcal{V}$.
- (3) For each $v \in \mathcal{V}$ the number of i such that $v \in B_i$ is even.

Let us show that the existence of a Kochen-Specker pair demonstrates the non-existence of a function f with the properties given above. Towards a contradiction suppose that $(\mathcal{V}, \mathcal{B})$ satisfies Definition 1.1 and $f : \mathbb{C}^n \rightarrow \{0, 1\}$ has the properties specified above. Denote $V_1 = \{x \in \mathcal{V} : f(x) = 1\}$. By conditions (2) and (3) and by properties of f , the number of i such that $|B_i \cap V_1| = 1$ is even. Since the length of the list \mathcal{B} is odd, there exists an i such that $|B_i \cap V_1| \neq 1$, in contradiction to the required properties of f . Since this contradiction is based on a parity argument, the Kochen-Specker pairs introduced in Definition 1.1 are often called “parity proofs of the Kochen-Specker theorem.”

It is quite common in the literature [2, 7, 9] to refer to a Kochen-Specker pair as *Kochen-Specker set*, and we will do so sometimes in this paper. Kochen-Specker sets are key tools for proving some fundamental results in quantum theory, and they also have various potential applications in quantum information processing [2]. In Section 3 we give a construction of a family of Kochen-Specker sets in infinitely many different dimensions. Before that, in Section 2 we introduce a new class of complex Hadamard matrices, which are used in our construction, and they may be also an interesting object of study on their own. In Section 4 we draw some conclusions from our results.

2 SL Hadamard matrices

For $z \in \mathbb{C}$ let \bar{z} denote its complex conjugate. We work with the usual inner product on \mathbb{C}^n defined by $\langle x, y \rangle = \sum_{i=1}^n x_i \bar{y}_i$. For a complex matrix H , let H^* denote its conjugate transpose. Let I_n denote the $n \times n$ identity matrix. We say that a complex number z is *unimodular* if $|z| = 1$. We say that a vector $x \in \mathbb{C}^n$ is *unimodular* if each coordinate of x is unimodular.

Definition 2.1. An $n \times n$ matrix $H = (h_{i,j})$ whose entries are complex numbers is called *SL Hadamard matrix of order n* if it meets the following conditions:

- (1) $HH^* = nI_n$
- (2) $|h_{i,j}| = 1$ for all $1 \leq i, j \leq n$
- (3) $h_{1,j} = 1$ for all $1 \leq j \leq n$
- (4) for each $1 \leq s, t \leq n$, $s \neq t$, we have $\sum_{j=1}^n h_{s,j}^2 h_{t,j} = 0$.

Conditions (1) and (2) are the definition of Hadamard matrices which are prominent objects in combinatorial design theory that have been studied since the 19th century [3], first as matrices over $\{-1, 1\}$ and then more generally as matrices over complex numbers. Any matrix that meets conditions (1) and (2) can be transformed to a matrix that meets condition (3) by, wherever necessary, multiplying all entries in a column by the inverse of the first entry in that column; this preserves conditions (1) and (2). By an analogous operation applied to rows, it is also possible to achieve that the first column of H consists entirely of ones; this is not required by our definition and our definition is compatible with this transformation. Hadamard matrices whose all entries in the first row and first column are 1 are usually called *normalized* (or “dephased”). While it is common but generally *not* required to write down Hadamard matrices in the normalized form, condition (3) of our definition *requires* that the first row of the matrix is normalized. Finally condition (4) appears to be a new condition not previously seen in the literature. The proposed name *SL Hadamard matrix* reflects the form of this new additional condition, which involves squares of the entries of a row, while the entries of another row are involved linearly. All four conditions in Definition 2.1 are required for our construction of Kochen-Specker pairs given in Theorem 3.1.

Throughout this paper we use additive notation for group operations.

Definition 2.2. [6, Definition 5.1] Let G be a group of order g and let λ be a positive integer. A *generalized Hadamard matrix* over G is a $g\lambda \times g\lambda$ matrix $M = (m_{i,j})$ whose entries are elements of G and for each $1 \leq k < \ell \leq g\lambda$, each element of G occurs exactly λ times among the differences $m_{k,j} - m_{\ell,j}$, $1 \leq j \leq g\lambda$. Such matrix is denoted $\text{GH}(g, \lambda)$.

Many constructions of $\text{GH}(g, \lambda)$ are known. Let \mathbb{Z}_m denote the cyclic group of integers modulo m . In Proposition 2.4 we use generalized Hadamard matrices over \mathbb{Z}_3 , therefore we will now list some cases for which $\text{GH}(3, \lambda)$ is known to exist. This list is by far not exhaustive.

Lemma 2.3. *For $t, u, v \geq 0$ there exist $\text{GH}(3, 2^t 3^u)$ and $\text{GH}(3, 2 \cdot 5^v)$. Furthermore if $t, u \geq 1$, $v \geq 0$ then there exists $\text{GH}(3, 2^t 3^u 5^v)$.*

Proof. By [6, Table 5.10] there exists $\text{GH}(3, 3^u)$ for $u \geq 0$. Then by [6, Theorem 5.12] (with $g = 3$, $\lambda = 1$) there exists $\text{GH}(3, 2^t)$ for $t \geq 0$, and by the same theorem (with $g = 3$, $\lambda = 2$) there exists $\text{GH}(3, 2 \cdot 5^v)$ for $v \geq 0$. If u is positive, then an application of [6, Theorem 5.11] to $\text{GH}(3, 2^t)$ and $\text{GH}(3, 3^{u-1})$ produces $\text{GH}(3, 2^t 3^u)$. Furthermore if $t, u \geq 1$, then an application of the same theorem to $\text{GH}(3, 2^{t-1} 3^{u-1})$ and $\text{GH}(3, 2 \cdot 5^v)$ produces $\text{GH}(3, 2^t 3^u 5^v)$. \square

Proposition 2.4. *Suppose that $\text{GH}(3, \lambda)$ over \mathbb{Z}_3 exists. Then there exists an SL Hadamard matrix of order 3λ .*

Proof. Assume that $M = (m_{i,j})$ is a $\text{GH}(3, \lambda)$. Without loss of generality we can assume that all entries in the first row of M are zeros. Let $\zeta_3 = e^{2\pi\sqrt{-1}/3}$ be the primitive cube root of unity in \mathbb{C} . Define the $(3\lambda) \times (3\lambda)$ matrix $H = (h_{i,j})$ by $h_{i,j} = \zeta_3^{m_{i,j}}$ for all i, j . We claim that H is an SL Hadamard matrix of order 3λ . Let h_s and h_t be two rows of H , $s \neq t$. Then

$$\langle h_s, h_t \rangle = \sum_{j=1}^{3\lambda} \zeta_3^{m_{s,j} - m_{t,j}} = \lambda(1 + \zeta_3 + \zeta_3^2) = 0$$

and $\langle h_s, h_s \rangle = \sum_{j=1}^{3\lambda} |h_{s,j}|^2 = 3\lambda$, thus condition (1) in Definition 2.1 is satisfied. Since $h_{s,j}^2 = h_{s,j}^{-1} = \overline{h_{s,j}}$ for all s, j by the construction of H , we also get

$$\sum_{j=1}^{3\lambda} h_{s,j}^2 h_{t,j} = \langle h_t, h_s \rangle = 0$$

which proves condition (4) in Definition 2.1. Conditions (2) and (3) in Definition 2.1 follow immediately from the construction of H . \square

It would be interesting to find other constructions of SL Hadamard matrices, and we pose this as an open problem.

3 An infinite family of Kochen-Specker sets

SL Hadamard matrices introduced in the previous section will now be used to construct an infinite family of Kochen-Specker sets.

Theorem 3.1. *Suppose that there exists an SL Hadamard matrix of order n where n is even. Then there exists a Kochen-Specker pair $(\mathcal{V}, \mathcal{B})$ in \mathbb{C}^n such that $|\mathcal{V}| \leq \binom{n+1}{2}$ and $|\mathcal{B}| = n + 1$.*

Proof. First we construct the set \mathcal{V} . Let the elements of \mathcal{V} be denoted $v^{\{r,s\}}$ where $1 \leq r, s \leq n+1$, $r \neq s$. Note that we use the standard convention that sets are unordered, hence $v^{\{r,s\}}$ and $v^{\{s,r\}}$ denote the same element of \mathcal{V} , for all $r \neq s$. For $x, y \in \mathbb{C}^n$ we define $x \circ y = (x_1 y_1, \dots, x_n y_n)$ and $\overline{x} = (\overline{x_1}, \dots, \overline{x_n})$.

Let $H = (h_{i,j})$ be the SL Hadamard matrix of order n whose existence is assumed, and let h_i denote the i -th row of H . We construct the elements of \mathcal{V} as follows:

- For $1 < s \leq n+1$ let $v^{\{1,s\}} = h_{s-1}$.
- For $2 < s \leq n+1$ let $v^{\{2,s\}} = \overline{h_{s-1}}$.
- For $2 < r < s \leq n+1$ let $v^{\{r,s\}} = h_{r-1} \circ h_{s-1}$.

For $1 \leq r \leq n+1$ let $B_r = \{v^{\{r,i\}} : 1 \leq i \leq n+1, i \neq r\}$, and let $\mathcal{B} = (B_1, \dots, B_{n+1})$. We will now prove that each B_r is an orthogonal basis of \mathbb{C}^n . Note that for $x, y, z \in \mathbb{C}^n$ such that z is unimodular we have

$$\langle z \circ x, z \circ y \rangle = \langle x \circ z, y \circ z \rangle = \sum_{i=1}^n x_i z_i \overline{y_i z_i} = \langle x, y \rangle. \quad (1)$$

Since distinct rows of H are orthogonal and all rows of H are unimodular, equation (1) proves

$$\langle v^{\{r,s\}}, v^{\{r,t\}} \rangle = 0 \quad (2)$$

whenever

$$2 < r, s, t \leq n+1 \text{ and } r, s, t \text{ are distinct.} \quad (3)$$

We will now prove the desired orthogonality relations (2) for those pairs of vectors $v^{\{r,s\}}, v^{\{r,t\}}$ which are not covered by condition (3). We will split the proof into cases according to the value of r .

Let $r = 1$. For $1 < s < t \leq n+1$ we have $\langle v^{\{1,s\}}, v^{\{1,t\}} \rangle = 0$ since distinct rows of H are orthogonal. Now let $r = 2$. For $2 < s < t \leq n+1$ we have

$$\langle v^{\{2,s\}}, v^{\{2,t\}} \rangle = \langle \overline{h_{s-1}}, \overline{h_{t-1}} \rangle = \langle h_{t-1}, h_{s-1} \rangle = 0.$$

Since $\overline{h_1} = h_1$, for $2 < t \leq n+1$ we have

$$\langle v^{\{2,1\}}, v^{\{2,t\}} \rangle = \langle h_1, \overline{h_{t-1}} \rangle = \langle h_{t-1}, h_1 \rangle = 0.$$

Finally let $2 < r \leq n+1$. Since h_1 is the row of all ones and all rows of H are unimodular, for $t > 2$, $t \neq r$ we have

$$\begin{aligned} \langle v^{\{r,1\}}, v^{\{r,t\}} \rangle &= \langle h_{r-1}, h_{r-1} \circ h_{t-1} \rangle = \langle h_{r-1} \circ h_1, h_{r-1} \circ h_{t-1} \rangle = \\ &= \langle h_1, h_{t-1} \rangle = 0 \end{aligned}$$

as well as

$$\begin{aligned}
\langle v^{\{r,2\}}, v^{\{r,t\}} \rangle &= \langle \overline{h_{r-1}}, h_{r-1} \circ h_{t-1} \rangle = \sum_{j=1}^n \overline{h_{r-1,j}} \overline{h_{r-1,j} h_{t-1,j}} = \\
&= \overline{\sum_{j=1}^n h_{r-1,j}^2 h_{t-1,j}} = 0
\end{aligned}$$

by condition (4) of Definition 2.1. Finally we have

$$\begin{aligned}
\langle v^{\{r,1\}}, v^{\{r,2\}} \rangle &= \langle h_{r-1}, \overline{h_{r-1}} \rangle = \sum_{j=1}^n h_{r-1,j} \overline{\overline{h_{r-1,j}}} = \\
&= \sum_{j=1}^n h_{r-1,j}^2 = \sum_{j=1}^n h_{r-1,j}^2 h_{1,j} = 0
\end{aligned}$$

again by condition (4) of Definition 2.1.

We note that $|\mathcal{B}| = n + 1$ is odd since n is assumed to be even. We will complete the proof by verifying that condition (3) in Definition 1.1 is satisfied. If the mapping $\{i, j\} \mapsto v^{\{i,j\}}$ is injective, then each $v^{\{i,j\}}$ belongs to exactly two entries of \mathcal{B} , namely B_i and B_j . If the list $(v^{\{i,j\}})_{1 \leq i < j \leq n+1}$ contains repeated vectors, then let x be a vector that occurs exactly t times in this list. Then by the previous argument x belongs to exactly $2t$ entries of \mathcal{B} , since $j \neq k$ implies $v^{\{i,j\}} \neq v^{\{i,k\}}$ as $\langle v^{\{i,j\}}, v^{\{i,k\}} \rangle = 0$. \square

Theorem 3.2. *Suppose that $n = 2^t 3^u$ where $t, u \geq 1$, or $n = 6 \cdot 5^v$ where $v \geq 0$, or $n = 2^t 3^u 5^v$ where $t \geq 1$, $u \geq 2$, $v \geq 0$. Then there exists a Kochen-Specker pair $(\mathcal{V}, \mathcal{B})$ in \mathbb{C}^n such that $|\mathcal{V}| \leq \binom{n+1}{2}$ and $|\mathcal{B}| = n + 1$.*

Proof. Suppose that n is of the form as required in the statement. By Lemma 2.3 there exists a GH(3, $n/3$) over \mathbb{Z}_3 . Then by Proposition 2.4 there exists SL Hadamard matrix of order $3 \cdot n/3 = n$. Since n is even by assumption, an application of Theorem 3.1 finishes the proof. \square

4 Conclusion

A Kochen-Specker pair $(\mathcal{V}, \mathcal{B})$ in \mathbb{C}^6 with $|\mathcal{V}| = 21$ and $|\mathcal{B}| = 7$ was recently discovered [7]. It was noted [2] as the *simplest* Kochen-Specker pair (KS pair) since it strictly minimizes the cardinality of \mathcal{B} among all known KS pairs $(\mathcal{V}, \mathcal{B})$, see [9]. This KS pair was originally found by computer search and its internal structure has not been fully studied yet. In this paper we have fully

revealed the structure of this KS pair, since it is obtained as the smallest instance ($n = 6$) of the infinite family characterized in Theorem 3.2. We have discovered an application of generalized Hadamard matrices to the construction of KS pairs, and we have proposed a new class of Hadamard matrices as the suitable domain for such constructions.

References

- [1] A. Cabello, A proof with 18 vectors of the Bell-Kochen-Specker theorem. In: M. Ferrero and A. van der Merwe (Eds.), *New Developments on Fundamental Problems in Quantum Physics*. Kluwer Academic, Dordrecht, Holland, 1997, pp. 59–62.
- [2] G. Cañas, M. Arias, S. Etcheverry, E.S. Gómez, A. Cabello, G.B. Xavier, G. Lima, Applying the simplest Kochen-Specker set for quantum information processing. *Phys. Rev. Lett.* **113** (2014), 090404.
- [3] K.J. Horadam, *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, NJ, 2007.
- [4] M. Howard, J. Wallman, V. Veitch, J. Emerson, Contextuality supplies the ‘magic’ for quantum computation. *Nature* **510** (2014), 351–355.
- [5] S. Kochen, E.P. Specker, The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* **17** (1967), 59–87.
- [6] W. de Launey, Generalized Hadamard matrices. In: C.J. Colbourn and J.H. Dinitz (Eds.), *Handbook of Combinatorial Designs*. Second edition. Chapman & Hall/CRC, Boca Raton, FL, 2007, pp. 301–306.
- [7] P. Lisoněk, P. Badziąg, J.R. Portillo, A. Cabello, Kochen-Specker set with seven contexts. *Physical Review A* **89** (2014), 042101.
- [8] M. Waegell, P.K. Aravind, Parity proofs of the Kochen-Specker theorem based on the Lie algebra E_8 . *J. Phys. A: Math. Theor.* **48** (2015), 225301.
- [9] M. Waegell, P.K. Aravind, The minimum complexity of Kochen-Specker sets does not scale with dimension. *arXiv:1702.05215 [quant-ph]* (Retrieved 28 February 2017)